Claims

WHAT IS CLAIMED IS:

1. A method of authenticating an identity of a user seeking access to a relying computing entity, wherein the identity of the user is issued by an authentication service and is not issued by the relying computing entity, the method comprising:

receiving at a broker service an authentication request from the relying computing entity to authenticate the identity of the user, wherein a first trust relationship exists between the relying computing entity and the broker service, and a second trust relationship exists between the authentication service and the broker service, in the absence of a relevant trust relationship existing between the authentication service and the relying computing entity;

receiving an authentication response from the authentication service, responsive to receiving the authentication request at the broker service; and

sending an authentication response from the broker service to the relying computing entity representing a trusted authentication of the identity of the user to the relying computing entity based on the first trust relationship and the second trust relationship.

2. The method of claim 1 further comprising:

sending the authentication request to the authentication service, responsive to receiving the authentication request at the broker service.

3. The method of claim 1 further comprising:

collecting a credential of the user, responsive to receiving the authentication request at the broker service; and

sending the credential to the authentication service for validation by the authentication service.

4. The method of claim 1 wherein the credential cannot be interpreted by the broker service.

5. The method of claim 1 wherein the broker service and the authentication service are hosted by a single computing system.

6. The method of claim 1 wherein the broker service and the authentication services are hosted within a single computing entity.

7. The method of claim 1 wherein authentication account information associated with the user and maintained by the authentication service is accessible through an interface to the authentication service.

8. The method of claim 1 further comprising:

validating based on the first trust relationship that the authentication request was received by the broker service from the relying computing entity.

9. The method of claim 1 wherein other computing entities have trust relationships established with the broker service.

10. The method of claim 1 wherein the first trust relationship represents an agreement between the broker service and the relying computing entity to comply with one or more brokered authentication rules.

11. The method of claim 1 wherein the first trust relationship represents an exchange of one or more security keys between the broker service and the relying computing entity.

12. The method of claim 1 wherein the first trust relationship represents an agreement by the relying computing entity to recognize assertions provided by the broker service.

13. The method of claim 1 wherein the operation of receiving at a broker service an authentication request is responsive to an access request by the user for access to the relying computing entity.

14. The method of claim 1 wherein the operation of receiving at a broker service an authentication request comprises:

receiving the authentication request at the broker service as a redirected message through a computer system of the user.

15. The method of claim 1 further comprising:

validating a credential received from the user by the authentication service.

16. The method of claim 1 further comprising:

sending a challenge request to the user, responsive to the operation of receiving at a broker service an authentication request; and

validating a credential received from the user in response to the challenge request.

17. The method of claim 1 further comprising:

returning a session ticket to the user to allow user access to the relying computing entity.

18. The method of claim 1 further comprising:

redirecting the user to the authentication service based on an identifier of the user.

19. The method of claim 1 further comprising:

translating the authentication response received from the authentication service into a protocol recognized by the relying computing entity.

20. A computer program product encoding a computer program for executing on a computer system a computer process for authenticating an identity of a user seeking access to a relying computing entity, wherein the identity of the user is issued by an authentication service, the computing process comprising:

receiving at a broker service an authentication request from the relying computing entity to authenticate the identity of the user, wherein a first trust relationship exists between the relying computing entity and the broker service, and a second trust relationship exists between the authentication service and the broker service;

receiving an authentication response from the authentication service; and

sending an authentication response from the broker service to the relying computing entity representing a trusted authentication of the identity of the user to the relying computing entity based on the first trust relationship and the second trust relationship.

21. The computer program product of claim 20 wherein the computer process further comprises:

sending the authentication request to the authentication service, responsive to receiving the authentication request at the broker service.

22. The computer program product of claim 20 wherein the computer process further comprises:

collecting a credential of the user, responsive to receiving the authentication request at the broker service; and

sending the credential to the authentication service for validation by the authentication service.

23. The computer program product of claim 20 wherein the credential cannot be interpreted by the broker service.

24. The computer program product of claim 20 wherein the broker service and the authentication service are hosted by a single computing system.

25. The computer program product of claim 20 wherein the broker service and the authentication services are hosted within a single computing entity.

26. The computer program product of claim 20 wherein authentication account information associated with the user and maintained by the authentication service is accessible through an interface to the authentication service.

27. The computer program product of claim 20 wherein the computer process further comprises:

validating based on the first trust relationship that the authentication request was received by the broker service from the relying computing entity.

28. The computer program product of claim 20 wherein other computing entities have trust relationships established with the broker service.

29. The computer program product of claim 20 wherein the first trust relationship represents an agreement between the broker service and the relying computing entity to comply with one or more brokered authentication rules.

30. The computer program product of claim 20 wherein the first trust relationship represents an exchange of one or more security keys between the broker service and the relying computing entity.

31. The computer program product of claim 20 wherein the first trust relationship represents an agreement by the relying computing entity to recognize assertions provided by the broker service.

32. The computer program product of claim 20 wherein the operation of receiving at a broker service an authentication request is responsive to an access request by the user for access to the relying computing entity.

33. The computer program product of claim 20 wherein the operation of receiving at a broker service an authentication request comprises:

receiving the authentication request at the broker service as a redirected message through a computer system of the user.

34. The computer program product of claim 20 wherein the computer process further comprises:

validating a credential received from the user by the authentication service.

35. The computer program product of claim 20 wherein the computer process further comprises:

sending a challenge request to the user, responsive to the operation of receiving at a broker service an authentication request; and

validating a credential received from the user in response to the challenge request.

36. The computer program product of claim 20 wherein the computer process further comprises:

returning a session ticket to the user to allow user access to the relying computing entity.

37. The computer program product of claim 20 wherein the computer process further comprises:

redirecting the user to the authentication service based on an identifier of the user.

38. The computer program product of claim 20 wherein the computer process further comprises:

translating the authentication response received from the authentication service into a protocol recognized by the relying computing entity.

39. A computer system for authenticating an identity of a user seeking access to a relying computing entity, wherein the identity of the user is issued by an authentication service, the computing system comprising:

an authentication broker service having a first trust relationship with the relying computing entity and a second trust relationship with the authentication service, the authentication broker service receiving an authentication request from the relying computing entity to authenticate the identity of the user and receiving an authentication response from the authentication service,

the authentication broker service further sending an authentication response to the relying computing entity representing a trusted authentication of the identity of the user to the relying computing entity based on the first trust relationship and the second trust relationship.

40. A method of establishing a brokerable trust relationship between an authentication broker service and each of a plurality of computing entities, the method comprising:

establishing one or more brokered authentication rules governing brokered authentication through the authentication broker service;

obtaining an agreement from each computing entity to comply with the one or more brokered authentication rules; and

configuring the authentication broker service to authenticate identities of one or more users for each computing entity in accordance with the one or more brokered authentication rules, wherein the one or more users have identities issued by one or more authentication services having trust relationships with the authentication broker service.

41. The method of claim 40 further comprising:

exchanging one or more security keys between the authentication broker service and each of the computing entities.

42. A computer program product encoding a computer program for executing on a computer system a computer process for establishing a brokerable trust relationship between an authentication broker service and each of a plurality of computing entities, the computer process comprising:

establishing one or more brokered authentication rules governing brokered authentication through the authentication broker service;

obtaining an agreement from each computing entity to comply with the one or more brokered authentication rules; and

configuring the authentication broker service to authenticate identities of one or more users for each computing entity in accordance with the one or more brokered authentication rules, wherein the one or more users have identities issued by one or more authentication services having trust relationships with the authentication broker service.

43. The computer program product of claim 42 wherein the computer process further comprises:

exchanging one or more security keys between the authentication broker service and each of the computing entities.